МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

программы подготовки специалистов среднего звена
по специальности СПО
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка 2023

- Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и с учётом профессиональных стандартов «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. № 536н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. № 533н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. № 525н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 9 августа 2022 г. № 474н.

.

Разработчик:

ОГАПОУ «Алексеевский колледж»	преподаватель	И.В. Косинова
(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. ОБЩЕЕ ПОЛОЖЕНИЕ

Контрольно-оценочные средства (далее – КОС) по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами является частью программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и предназначен для оценки результатов освоения профессионального модуля. Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида деятельности - Защита информации в автоматизированных системах программными и программно-аппаратными средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ППССЗ в целом.

Форма промежуточной аттестации по ПМ – экзамен по модулю.

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

Условием допуска к экзамену по модулю является успешное освоение обучающимися всех элементов программы профессиональных модулей: программ МДК 02.01. Программные и программно-аппаратные средства защиты информации и , учебной и производственной практики.

Формы промежуточной аттестации по профессиональному модулю

Таблица 1.

Элемент модуля	**Форма контроля и оценивания**	
	Промежуточная аттестация	**Текущий контроль**
МДК 02.01. Программные и программно-аппаратные средства защиты информации	Экзамен	Экспертная оценка в рамках текущего контроля на теоретических и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
МДК 02.02 Криптографические средства защиты информации	Экзамен	Экспертная оценка в рамках текущего контроля на теоретических и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
УП.02. Учебная практика	Дифференцированный зачет	Экспертная оценка в рамках текущего контроля в ходе проведения учебной

		практики.
ПП.02 Производственная практика	Дифференцированный зачет	Экспертная оценка в рамках текущего контроля в ходе проведения производственной практики.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

2.1. Профессиональные и общие компетенции

Целью экзамена по модулю является комплексная проверка готовности к овладению обучающимися видом деятельности и сформированности у них основных профессиональных и общих компетенций по запланированным показателям оценки результата.

Результатом освоения профессионального модуля является овладение обучающимися видом деятельности - Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе общими компетенции (ОК) и профессиональными компетенциями (ПК):

Таблица 2.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Уметь распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника). Знать актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Уметь определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска. Знать номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие	Уметь определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития Знать содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
ОК 04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Уметь организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами Знать психология коллектива; психология личности; основы проектной деятельности
ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Уметь излагать свои мысли на государственном языке; оформлять документы. Знать особенности социального и культурного контекста; правила оформления документов.
ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	Уметь описывать значимость своей профессии Презентовать структуру профессиональной деятельности по специальности Знать сущность гражданско-патриотической позиции Общечеловеческие ценности Правила поведения в ходе выполнения профессиональной деятельности
ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Уметь соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности. Знать правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения.
ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	Уметь использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности Знать роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.

ОК 09 Использовать информационные технологии в профессиональной деятельности	Уметь применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение Знать современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках	Уметь понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы Знать правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

2.2. Портфолио как контрольно-оценочное средство профессионального модуля

Портфолио обучающихся ОГАПОУ «Алексеевский колледж» - это комплекс документов (грамоты, дипломы, сертификаты, копии приказов, фотодокументы и т.д.), отзывов и продуктов различных видов деятельности: как учебной (диагностические работы, научно-исследовательские и проектные работы, рефераты, результаты самостоятельной работы и т.д.), так и внеурочной (творческие работы, презентации, фото и видеоматериалы).

Портфолио может содержать материал из внешних источников (отзывы или грамоты, выписки из приказов с практики, с военных сборов и т.д.), дающий дополнительную оценку освоения общих и профессиональных компетенций.

Портфолио является контрольно-оценочным средством профессионального модуля (ПМ) и позволяет оценить сформированность общих и профессиональных компетенций.

Портфолио создается в течение всего обучения в колледже. Портфолио в дальнейшем может служить основой для составления резюме выпускника при поиске работы, при продолжении образования и др.

Цель Портфолио: отслеживание и оценивание формирования общих и профессиональных компетенций в рамках освоения программы подготовки

специалистов среднего звена среднего профессионального образования (ППССЗ СПО).

Задачи Портфолио: отслеживание персональных достижений обучающихся в соответствии с поэтапными требованиями ППССЗ СПО; оценивание сформированности общих компетенций ППССЗ СПО; оценивание сформированности профессиональных компетенций ППССЗ СПО; оценивание освоения видов профессиональной деятельности в соответствии с ФГОС СПО специальности; формирование и совершенствование учебной мотивации, мотивации достижений и мотивации на профессиональную деятельность.

Функции Портфолио: - функция предъявления, фиксации и накопления документально подтвержденных персональных достижений в процессе освоения ОПОП; - функция оценивания сформированности общих и профессиональных компетенций; - функция экспертной оценки освоения видов профессиональной деятельности; - функция формирования личной ответственности за результаты учебно- профессиональной деятельности,

профессионально-личностного самосовершенствования, мотивации и интереса.

Участниками работы над портфолио являются студенты, преподаватели, кураторы. Одним из основных условий составления портфолио является установка тесного сотрудничества между всеми участниками и четкое распределение обязанностей между ними.

Обязанности студента: оформляет Портфолио в соответствии с принятой в ОГАПОУ «Алексеевский колледж» структурой; систематически самостоятельно пополняет соответствующие разделы материалами, отражающими успехи и достижения в учебной, производственной и внеучебной деятельности; отвечает за достоверность представленных материалов; при необходимости обращается за помощью к куратору.

Обязанности куратора: направляет всю работу студента по ведению портфолио, консультирует, помогает, дает советы, объясняет правила ведения и заполнения портфолио; совместно со студентами отслеживает и оценивает динамику их индивидуального развития и профессионального роста, поддерживает их образовательную, профессиональную, творческую активность и самостоятельность; выполняет роль посредника между студентом, преподавателями, обеспечивает их постоянное сотрудничество и взаимодействие; осуществляет контроль за заполнением соответствующих разделов Портфолио; помогает сделать электронные копии приказов, распоряжений и т.д. администрации колледжа и внешних организаций.

Обязанности преподавателей: преподаватели проводят экспертизу и оценку представленных работ по дисциплине, междисциплинарному курсу, профессиональному модулю и дают рекомендацию о размещении работы в портфолио (допускается размещение работ, выполненных на оценку не ниже «хорошо»), оформляют сертификат установленного образца; преподаватели/сотрудники администрации, являющиеся организаторами проведения различных мероприятий в колледже оформляют сертификат установленного образца на участие студента в тех или иных мероприятиях;

оформляют заявку на имя заведующего отделением для поощрения студентов за участие в учебной и внеучебной работе: грамоты, дипломы, отзывы, благодарности.

Обязанности администрации: заведующий отделением, руководитель практики, заместители директора по учебной работе, учебно-методической работе, учебно- производственной работе, воспитательной работе, методист осуществляют общий контроль за деятельностью педагогического коллектива по реализации технологии портфолио и оказывают необходимую помощь кураторам в организации сбора документов соответствующих разделов портфолио; собеседование с лицами, поступающими в колледж; по итогам учебного года организует награждение Почетными грамотами лучших студентов в номинациях: за успехи в учебе, за активное участие в общественной работе, за активное участие в культурно-массовой работе, за активное участие в военно-патриотической работе, за активное участие в волонтерском движении и т.д.

Ведение портфолио осуществляется самим студентом в печатном (папка-накопитель с файлами) и электронном виде. Каждый отдельный материал, включенный в портфолио за время обучения в образовательном учреждении, датируется.

Структура портфолио:

1) Титульный лист.

2) Раздел «Официальные документы».

3) Достижения в освоении образовательной программы и программ дополнительного образования. В этом разделе помещаются все имеющиеся у студента сертифицированные документы, подтверждающие его индивидуальные достижения: копии документов (свидетельств), подтверждающих обучение по основной образовательной программе и программам дополнительного образования; информация о наградах, грамотах, благодарственных письмах; копии документов (свидетельств), подтверждающих его участие в различных конкурсах (соревнованиях и т.д.); другие документы по усмотрению автора.

4) Раздел «Итоги прохождения производственной практики» формируется по мере прохождения студентом производственной практики по профессиональным модулям, предусмотренным ППССЗ по специальностям. Формирование данного раздела является обязательным требованием для каждого студента. Раздел включает в следующие материалы: характеристики с места прохождения практики, заверенная подписью общего руководителя производственной практики и печатью учреждения; отзывы, благодарности от руководителей практик, руководства организаций, где студент проходил производственную практику; аттестационные листы.

5) Раздел «Достижения в НИРС и УИРС» формируется в период всего обучения студента в колледже. В данном разделе допускается представление копий документов. Радел включает следующие материалы: исследовательские работы и рефераты; отзывы на курсовые работы и проекты (возможно в электронном виде); ксерокопии статей или печатные издания со статьями

студента; тезисы докладов на конференциях, семинарах и т.д.; все имеющиеся у студента сертифицированные документы, подтверждающие индивидуальные достижения в различных видах деятельности: дипломы об участии в предметных олимпиадах и конкурсах профессионального мастерства, научно-практических конференциях различного уровня, грамоты за участие в конкурсах, сертификаты прохождения курсов дополнительного образования и т.д.

6) Раздел «Дополнительные личные достижения» формируется в период всего обучения студента в колледже. В данный раздел включаются работы и сертифицированные документы, подтверждающие индивидуальные достижения в области искусства, творчества, волонтерства, спорта или официальные документы, подтверждающие участие, достижения во внеучебной деятельности.

При оформлении портфолио необходимо соблюдать следующие требования: оформлять в печатном виде отдельными листами формата А4 (в пределах одного бланка или листа, таблицы); предоставлять достоверную информацию; располагать материалы в папке Портфолио в соответствии с принятой в ОГАПОУ «Алексеевский колледж» структурой портфолио. Студент самостоятельно оформляет Разделы. Преподаватель и куратор периодически контролируют и проверяют достоверность информации. Ответственность за сохранность подлинных документов и материалов несет лично студент. На экзамен (квалификационный) по профессиональному модулю студент обязан предоставить подлинные подтверждения своих профессиональных достижений.

3. ОСВОЕНИЕ ЗНАНИЙ, УМЕНИЙ, ПРАКТИЧЕСКОГО ОПЫТА

3.1. Комплект материалов для оценки сформированности знаний, умений, практического опыта по МДК 02.01. Программные и программно-аппаратные средства защиты информации и МДК 02.02 Криптографические средства защиты информации

Комплект оценочных средств предназначен для оценки результатов освоения МДК 02.01. Программные и программно-аппаратные средства защиты информации и МДК 02.02 Криптографические средства защиты информации в рамках текущей и промежуточной аттестации.

Форма промежуточной аттестации – Экзамен.

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

иметь практический опыт:

О1 установки, настройки программных средств защиты информации в автоматизированной системе;

О2 обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

О3 тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;

О4 решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

О5 применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

О6 учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

О7 работы с подсистемами регистрации событий;

О8 выявления событий и инцидентов безопасности в автоматизированной системе.

уметь:

У.1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных;

У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У.6 применять математический аппарат для выполнения криптографических преобразований;

У.7 использовать типовые программные криптографические средства, в том числе электронную подпись;

У.8 применять средства гарантированного уничтожения информации;

У.9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У.10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

знать:

З.1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З.2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З.6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Критерии оценки результатов освоения МДК 02.01. Программные и программно-аппаратные средства защиты информации и МДК 02.02 Криптографические средства защиты информации:

– **«5» «отлично» или «зачтено»** – студент показывает глубокое и полное овладение содержанием программного материала по МДК, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

– **«4» «хорошо» или «зачтено»** – студент в полном объеме освоил программный материал по МДК, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

– **«3» «удовлетворительно» или «зачтено»** – студент обнаруживает знание и понимание основных положений программного материала по МДК но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

– **«2» «неудовлетворительно» или «не зачтено»** – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и

неуверенно излагает программный материал по МДК, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. 2. Типовые задания для оценки освоения МДК 02.01. Программные и программно-аппаратные средства защиты информации и МДК 02.02 Криптографические средства защиты информации

3.2.1. Комплект оценочных средств для текущей аттестации по МДК 02.01. Программные и программно-аппаратные средства защиты информации

Практические задания (ПЗ)

ПЗ №1 Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов
ПЗ №2 Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.
ПЗ №3 Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.
ПЗ №4 Управление политикой безопасности. Шаблоны безопасности
Криптографическая защита. Обзор программ шифрования данных
Управление политикой безопасности. Шаблоны безопасности
ПЗ №5 Распределение каналов в соответствии с источниками воздействия
ПЗ №6-7 Организация доступа к файлам
Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД
ПЗ №8-9 Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО
ПЗ №10 Защита информации от несанкционированного копирования с использованием специализированных программных средств
ПЗ № 11. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)
ПЗ №12. Применение средства восстановления остаточной информации на примере Foremost или аналога
ПЗ №13. Применение специализированного программно средства для восстановления удаленных файлов
ПЗ №14. Применение программ для безвозвратного удаления данных
ПЗ №15. Применение программ для шифрования данных на съемных носителях
ПЗ №16. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений
ПЗ №17 Развертывание VPN
ПЗ №18 Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.
ПЗ № 19. Изучение различных способов закрытия "опасных" портов

ПЗ №20. Изучение механизмов защиты СУБД MS Access
ПЗ № 1. Изучение штатных средств защиты СУБД MSSQL Server.
ПЗ №22. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов
ПЗ № 23. Проведение аудита ЛВС сетевым сканером.
ПЗ №24 Выбор мер защиты информации для их реализации в информационной системе. ПЗ №25 Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке

3.2.2. Комплект оценочных средств для текущей аттестации по МДК 02.02. Криптографические средства защиты информации

Практические задания (ПЗ)

ПЗ №1. Методы замены и перестановки.

Форма контроля –письменный контроль.

Задание.Порядок выполнения работы.

1.Повторить краткие теоретические сведения о шифрах замены и перестановки.

2. Зашифровать открытый текст: Standardofsecurity с помощью шифра простой замены над латинским алфавитом.

3. Исходя из распределения вероятностей знаков английского языка, составить шифратор и дешифраторшифра многозначной пропорциональной замены (на 100 цифровых шифробозначений).

4. Зашифровать открытый текст ThereareseveraldailytrainstoBrightonc помощью шифра Виженеранад латинским алфавитом с произвольно выбранным разовым ключом.

5. С помощью одноразового шифровального блокнота зашифровать на ключе, представляющем собой последовательность случайных чисел, произвольный открытый текст длиной не менее 23-х символов на любом европейском языке.

6. Зашифровать шифром вертикальной перестановки с ключом длины 7 произвольный открытый текст длиной не менее 50-и символов на любом европейском языке.

7. Составить отчет, приобщив полученные результаты.

Требования к отчёту. В отчёте должны быть приведены: Краткие теоретические сведения о шифрах замены и перестановки. Открытые сообщения. Зашифрованные (расшифрованные) сообщения. Описание выбранных ключей.

ПЗ №2 Комбинированные методы шифрования

.Форма контроля –письменный контроль.

Задание: Задание на лабораторную работу. В лабораторной работе необходимо зашифровать по алгоритмуDES-ECBсообщение, состоящее из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени.

В качестве ключа выбрать первые 7 букв шифруемого сообщения

.При оформлении отчета необходимо привести:

- шифруемое сообщение (8 букв фамилии) в символьном и битовом представлении в соответствии скодировкой Windows 1251;
- ключ (7 букв фамилии) в символьном и битовом представлении в соответствии скодировкой Windows1251 ;
- ключ в битовом представлении с учетом битов контроля четности;
- ключевые элементы ki.

Оформить отчет по лабораторной работе.

ПЗ № 3

Шифрование методами замены

Форма контроля –письменный контроль.

Задание.Зашифровать свою фамилию имя отчество следующимиподклассами

Метода замены:

- шифры однозначной замены;
- полиграммные шифры;
- омофонические шифры;
- полиалфавитные шифры.

Оформить отчет по лабораторной работе.

ПЗ № 4 Таблица Виженера

Форма контроля –письменный контроль.

Задание Необходимо расшифровать данный текст, используя таблицу Виженера.

Текст:

LoatuvftYejeerzAgibeejwzriyazfrkknxefvoxvhanvmsxlizyjzhnxmvhnjwyhnonafjgmiunfrbjxnzrrgfkgearfywv.Bnotfrqgwesiprqzbvotvvgomcumozbklszuqzsypizhslbjtmkngrzggdgpccwkwsiireqk,tsceycoyvuztveukwgktrtvthlugvvgggdonafjgmibengdxhaihrj.HnxUtiivfybte’scfgomiunvehnxngtvfbgeutiivfybterneyoggypefjoweyprigatsovrvjowetcrkcomsgcuzsbxmkngj,ovhsotvmsofamenergiaysvfblhrkxpvzrxnie:FWsjNwgsnnoxwejtuv5hnilgcrzbzaeGnalorBnjecvbjxnzNnkwugarUazjkksotlIotditgf.JTkwUkqhzdybtygerrattksjzhnxsyeakwgesqiycgzhgovrkvkfaiozgszbtovrrrbtnzatvknxnotpfakltugrkhogggjbs.HnxktojcsjzegcdlwxxdgtFWsjNetaocsymhkmgfpuedrysrqkmhkdrdotwsgnqtvgelkntvguytne21fkqkgtarlrgcxlrafkcihnzrvsizxtutuvrkoerocdstmoltuvzuvarcbdaagiz

ПЗ №5

Шифрование информации методами сложной замены.

Форма контроля –письменный контроль.

Задание.Реализуйте шифрование методами сложной замены (шифр Гронсфельда)данный текст.

Текст: Шифры сложной замены называют многоалфавитными шифрами, в таких шифрах для преобразования каждого отдельно взятого

элемента естественного алфавита применяют свой шифр простой замены, устраняя при этом статистические демаскирующие признаки.

Код (19076729).

Провести дешифрацию.

Оформить отчет.

ПЗ № 6 Изучение дешифрования методом частотного анализа для шифров замены.

Форма контроля –письменный контроль.

Задание1.Разработать алгоритм для шифрования сообщений по лиалфавитным шифром Виженера.

2.Разработать алгоритм для дешифрования сообщений зашифрованных полиалфавитным шифром Виженера.

3.Составить приложение для шифрования/дешифрования с использованием полиалфавитным шифром Виженера с кодовым словом заданной длины.

Оформить отчет по лабораторной работе

ПЗ № 7 Применение сочетаний символов различных кодовых алфавитов.

Форма контроля –письменный контроль.

Задание. Закодировать методом Хаффмена название данного МДК(Криптографические средства и методы защиты информации).Рассчитать среднюю длину кодовой комбинации и ее минимальное значение.

Оформить отчет по лабораторной работе.

Контрольные вопросы.

1.Принцип формирования кодовых комбинаций при кодировании методом Хаффмена.

2.Как рассчитывается средняя длина кодовой комбинации кода Хаффменаи каково ее минимальное значение?

3.В чем состоит свойство префиксности эффективных кодов?

4.Количественные показатели эффективности неравномерного кодирования.

5.Принцип декодирования последовательности префиксного кода.

6.Принципы возникновения трека ошибок при декодировании последовательности кодовых комбинаций префиксного кода

ПЗ № 8 Основы компьютерных методов шифрования информации по таблице ASCII-кодов.

Форма контроля –письменный контроль.

Задание.1.Закодируйте следующие слова, используя таблицы ASCII-кодов: ИНФОРМАТИЗАЦИЯ, МИКРОПРОЦЕССОР, МОДЕЛИРОВАНИЕ

2.Раскодируйте следующие слова, используя таблицы ASCII-кодов: 88 AD E4 AE E0 AC A0 E2 A8 AA A050 72 6F 67 72 61 6D43 6F 6D 70 75 74 65 72

20 49 42 4D 20 50 43

Оформить отчет по лабораторной работе

ПЗ № 9

Симметричные системы шифрования.

Форма контроля –письменный контроль. Задание. Варианты заданий: Шифрование и расшифровка текста комбинацией двух разных из нижеуказанных методов. Программа должна для каждого символа (или блока) исходного файла произвольной структуры (.exe, .txt) применить первый метод, затем второй и только затем записать ввыходной файл. Для методов, требующих ключа определенного вида, например для перестановок, ключ должен формироваться на основании одного произвольного ключа, задаваемого пользователем. Пример ключа: фф12К52. Зашифрованный и дешифрованный файлы по возможности должны иметь размер исходного файла.

ПЗ 10

Односторонние хеш-функции.

Для создания подписи сообщения Мотправитель

1.вычисляет хеш-образ r= h(M) сообщения Мс помощью некоторой хеш-функции

;2.зашифровывает полученный хеш-образ rна своем секретном ключе (d,n) , т.е. вычисляет значение s= rdmodn,которое и является подписью.

Пример. Создать хеш–образ слова «КОЗИНА», используя хеш–функцию

□□2ii 1iHHMmod n□□□, где n= pq, p=13, q=19.

Хешируемое сообщение «КОЗИНА». Возьмем два простых числа p=13, q=19 Определим n=pq=13*19=247.

Вектор инициализации 0Нвыберем равным 8 (выбираем случайным образом).

Слово «КОЗИНА» можно представить последовательностью чисел (12, 16, 9, 10, 15, 1) по номерам букв в алфавите. Таким образом,

n=247, H0=8, M1=12, M2=16, M3=9, M4=10, M5=15, M6=1.

Используя формулу□□2ii 1iHHMmod n□□□,получим хеш-образ сообщения

«КОЗИНА»:H1=(H0+M1)2mod

n = (8+12)2mod247=400 mod 247=153H2=(H1+M2)2mod

n = (153+16)2mod247=28561mod 247= 156H3=(H2+M3)2mod

n = (156+9)2mod247=27225mod 247= 55H4=(H3+M4)2mod

n = (55+10)2mod247=4225mod 247= 26H5=(H4+M5)2mod

n = (26+15)2mod247=1681mod 247= 199

9H6=(H5+M6)2mod

n = (199+1)2mod247=40000mod 247= 233

В итоге получаем хеш-образ сообщения «КОЗИНА», равный 233

ПЗ 11

Шифрование с открытым ключом

.Форма контроля –письменный контроль.

Задание:Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;
- алгоритма на основе задачи об укладке ранца;
- алгоритма шифрования Эль-Гамаля.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования.

Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго –в соответствии скодировкой Windows 1251.

3.2.3. Комплект оценочных средств для промежуточной аттестации по МДК.02.01 Программные и программно-аппаратные средства защиты информации

Контрольные вопросы (КВ)

КВ № 1. Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации
КВ № 2. Классификация методов и средств программно-аппаратной защиты информации.
КВ № 3. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)
КВ № 4. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
КВ № 5. Автоматизация процесса обработки информации. Понятие автоматизированной системы. Методы создания безопасных систем
КВ № 6. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.
КВ № 7. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели
КВ № 8. Источники дестабилизирующего воздействия на объекты защиты. Причины и условия дестабилизирующего воздействия на информацию
КВ № 9. Способы воздействия на информацию. Понятие несанкционированного доступа к информации
КВ № 10. Основные подходы к защите информации от НСД
КВ № 11. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса
КВ № 12. Особенности защиты данных от изменения. Шифрование.
КВ № 13. Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды.
КВ № 14. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.
КВ № 15. Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение
КВ № 6. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям.

КВ № 17. Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
КВ № 18. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.
КВ № 19. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме"
КВ № 20. Основные концепции построения систем антивирусной защиты на предприятии. Несанкционированное копирование программ как тип НСД
КВ № 21. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.
КВ № 22. Привязка ПО к аппаратному окружению и носителям. Проблема защиты отчуждаемых компонентов ПЭВМ.
КВ № 23. Защитные механизмы в современном программном обеспечении на примере MS Office.
КВ № 24. Методы защиты информации на отчуждаемых носителях. Шифрование.
КВ № 25. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
КВ № 26. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов
КВ № 27. Безвозвратное удаление данных. Принципы и алгоритмы.
КВ № 28. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
КВ № 29. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ
КВ № 30. Использование сетевых снифферов в качестве СОВ
КВ № 31. Аппаратный компонент СОВ. Программный компонент СОВ.
КВ № 32. Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.
КВ № 33. Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP.
КВ № 34. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.
КВ № 35. Виртуальная частная сеть. Функции, назначение, принцип построения
КВ № 36. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
КВ № 37. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Методы защиты информации при работе в сетях общего доступа.
КВ № 38. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall.

КВ № 39. Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня.
КВ № 40. Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов.
КВ № 41. Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом Средства контроля целостности информации в базах данных
КВ № 42. Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных
КВ № 43. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации
КВ № 44. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25
КВ № 45. Классификация отслеживаемых событий. Особенности построения систем мониторинга
КВ № 46. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов
КВ № 47. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.
КВ № 48. Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.

Тестовые задания (ТЗ)

Тест на тему «Программно–аппаратные средства обеспечения информационной безопасности»

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность
- Доступность
- Актуальностl

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности

+ Аудит, анализ уязвимостей, риск-ситуаций

29) Ценность информации определяется:

- a) степенью ее полезности для владельца
- b) истинностью или достоверностью
- c) конфиденциальностью

30) Объектом защиты информации является:

- a) работа, посвященная защите информации в автоматизированных системах
- b) компьютерная система или автоматизированная система обработки данных
- c) комплекс средств, предназначенных для автоматизированного сбора

31) Компьютерная система- это...

- a) вычислительные комплексы и системы
- b) вычислительные сети
- c) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации

32) Под системой защиты информации в КС понимается:

- a) состояние всех компонент компьютерной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне
- b) одно из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы
- c) единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

33) Сеть ЭВМ - это...

- a) процессы сбора, обработки, накопления, хранения, поиска и распространения информации
- b) это совокупность ЭВМ, взаимосвязанных каналами передачи данных, и необходимых для реализации этой взаимосвязи программного обеспечения и (или) технических средств, предназначенных для организации распределенной обработки данных
- c) информация, возникающая в ходе ведения разговоров, работы систем связи, звуко - усиления и звуковоспроизведения

34) Под информационной системой понимают:

- a) упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы
- b) процессы сбора, обработки, накопления, хранения, поиска и распространения информации
- c) информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче

35) Информационными ресурсами называют:

- a) процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом
- b) документы и массивы документов, существующие отдельно или в составе информационных систем
- c) государственные тайны и конфиденциальную информацию

36) Разглашение - это...

- a) доведение защищаемой информации до неконтролируемого количества получателей информации
- b) получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней

- c) деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

37) Несанкционированное воздействие на защищаемую информацию - это…

- a) предотвращение ущерба собственнику, владельцу или пользователю информации
- b) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации
- c) воздействие с нарушением правил ее изменения

38) Шифрованием информации называют:

- a) процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- b) известность ее содержания только имеющим соответствующие полномочия субъектам
- c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации

39) Политика безопасности - это...

- a) состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
- b) это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа
- c) это известность ее содержания только имеющим соответствующие полномочия субъектам

40) Контроллер - это...

- a) основное устройство системы, производящее идентификацию пользователя и дающее разрешение на проход, в случае если считанный с идентификатора код совпадает с кодом, хранящимся в памяти контроллера
- b) это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа
- c) это известность ее содержания только имеющим соответствующие полномочия субъектам

41) Основной характеристикой контроллера являются:

- a) комбинированные методы
- b) поддерживаемые режимы работы - автономный или сетевой через линию связи с использованием компьютера
- c) при помощи особых устройств, генерирующих модулированный ультразвуковой, инфракрасный или радиосигнал

42) Идентификация - это...

- a) пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе
- b) информационных ресурсов, систем и технологий является субъект с полномочиями владения и пользования указанными объектами. Под пользователем информации будем понимать субъекта, обращающегося к информационной системе за получением необходимой ему информации и пользующегося ею
- c) пользователь сообщает системе по ее запросу свое имя

43) Основной недостаток подобных систем аутентификации:

- a) информацией в данном случае служит ключ, на котором выполняется шифрование случайного числа. Как видно из схемы обмена, данный ключ никогда не передается по сети, а лишь участвует в вычислениях, что составляет несомненное преимущество протоколов данного семейства

- b) необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование
- c) сервер расшифровывает полученную информацию на том же ключе и сравнивает с исходным случайным числом

44) Самый главный недостаток протокола Kerberos:

- a) необходимость в нескольких специальных серверах
- b) В случае успешной проверки билета сервер TGS генерирует еще один случайный ключ для шифрования сеансов связи между пользователем, желающим получить доступ, и целевым сервером
- c) необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование

45) Выбрать правильный ответ, характеризующий протокол идентификации CHAP:

- a) проверяющая система отправляет запрос удаленному устройству, которое запросило подключение к сети
- b) применяет простую процедуру двустороннего обмена для идентификации систем
- c) использует специальный алгоритм для расчета значения, известного только проверяющей системе и удаленному устройству

46) Хешированием информации называют

- a) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации
- b) состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
- c) процесс ее преобразования в хеш -значение фиксированной длины

47) Множество объектов и типов доступа к ним субъекта может изменяться:

- a) в соответствии с некоторыми правилами, существующими в данной системе
- b) статично т.е. не может изменяться вообще
- c) это никак не связано с субъектами

48) Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

- a) все субъекты и объекты системы должны быть идентифицированы
- b) права доступа субъекта к объекту системы определяются без правил
- c) все субъекты и объекты системы должны быть не аутентифицированы

49) Избирательное управление доступом:

- a) концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности
- b) метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит
- c) в метод управления доступом субъектов системы к объектам, основанный на опознавании пользователя без любой регистрации

50) Мандатное управление доступом:

- a) метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит
- b) метод доступа субъектов к информационным ресурсам с полной разрешенностью к пользованию информаци
- c) концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности

51) Матрица доступа представляет собой:

- a) прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец

- b) треугольную матрицу, в которой объекту системы соответствует столбец, а субъекту строка
- c) квадратную матрицу, в которой объекту системы соответствует строка, а субъекту столбец

52) Избирательная политика безопасности наиболее широко применяется:

- a) в социальном секторе
- b) в коммерческом секторе
- c) в секторе политики

53) Какие виды резервного копирования поддерживает программа Handy Backup? Выберите несколько вариантов ответа.

a) Полное ✔
b) Выборочное
c) Рабочее
d) Инкрементальное ✔
e) Смешанное ✔
f) Дифференциальное ✔
g) Системное
h) Пользовательское

54) Какие из названных систем резервного копирования являются российскими?

a) Киберпротект ✔
b) Handy Backup ✔
c) Acronis
d) RuBackup ✔
e) Bacula

55) Бесплатная лечащая утилита от российского производителя антивирусов называется:

a) Spider
b) CureIt! ✔
c) Katana
d) vxCube

56) Какой антивирусный продукт Лаборатории Касперского является базовым?

a) Kaspersky Total Security
b) Kaspersky Anti-Virus
c) Kaspersky Internet Security ✔
d) Kaspersky Secure Connection
e) Kaspersky Safe Kids

57) Криптопровайдер это:

a) Компания, реализующая услугу оформления ЭЦП
b) Специальное ПО, реализующее все криптографические алгоритмы ✔
c) Программа, позволяющая формировать пары логин-пароль
d) Удостоверяющий центр, продает токены

58). Простая электронная подпись представляет собой:

a) Аналог собственноручной подписи
b) Выдается аккредитованным удостоверяющим центром
c) Логин и пароль ✔
d) Две уникальные последовательности символов, которые однозначно связаны между собой

59) Санкционированное воздействие на защищаемую информацию - это…

a) предотвращение ущерба собственнику, владельцу или пользователю информации
b) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации
c) воздействие с не нарушением правил ее изменения

60) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность Актуальность
- Доступность. Понятность

Критерии оценки:

Оценка	Процент выполнения заданий теста
5	85
4	70
3	50
2	Менее 50

3.2.4. Комплект оценочных средств для промежуточной аттестации по МДК 02.02 Криптографические средства защиты информации

Контрольные вопросы (КВ)

КВ 1. Перечислите и кратко охарактеризуйте основные задачи обеспечения информационной безопасности, решаемые с помощью криптографических методов.
КВ 2. Раскройте определения: шифрование, зашифрование, расшифрование, дешифрование.
КВ 3. Чем шифрование отличается от кодирования?
КВ 4. Приведите известные вам классификации криптосистем.
КВ 5. Укажите основные отличия между современной и классической криптографией.
КВ 6. Сравните аффинный шифр и шифр Хилла с точки зрения криптостойкости.
КВ 7. Опишите способы криптоанализа.
КВ 8. Сравните криптосистему RSA и криптосистему Эль-Гамаля.
КВ 9. Укажите основной недостаток кодов аутентичности сообщений.
КВ 10. Дайте понятие криптографического протокола.
КВ 11. Укажите основные отличия между современными и классическими блочными шифрами.
КВ 12. Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?
КВ 13. Сравните DES и ГОСТ 28147-89.

КВ 14. Сравните AES и ГОСТ 28147-89.
КВ 15. Перечислите основные свойства хеш-функций.
КВ 16. Чем хеширование отличается от выработки контрольных сумм?
КВ 17. Чем хеширование отличается от выработки имитовставки?
КВ 18. Укажите два подхода к построению функций хеширования.
КВ 19. Основные методы криптоанализа. Криптографические атаки.
КВ 20. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса
КВ 21. Перспективные направления криптоанализа, квантовый криптоанализ.
КВ 22. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии
КВ 23. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.

Тестовые задания (ТЗ)

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

4. ОЦЕНКА ПО УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

4.1. Общие положения

Комплект оценочных средств предназначен для оценки результатов освоения учебной и производственной практик профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Целью текущей и промежуточной аттестации по учебной и производственной практике является комплексная проверка сформированности у обучающихся практических профессиональных умений и навыков в рамках профессионального модуля по основному виду деятельности - Разработка, администрирование и защита баз данных для освоения профессии, обучения трудовым приемам, операциям и способам выполнения трудовых процессов, характерных для соответствующей профессии и необходимых для последующего освоения ими общих и профессиональных компетенций по избранной специальности.

4.2. Виды работ практики и проверяемые результаты обучения по профессиональному модулю

4.2.1. Учебная практика:

Таблица 4

№ п/п	Виды учебной работы на практике, включая	Проверяемые результаты (ПК, ОК, ПО, У)	Форма проверки результато

	самостоятельную работу студентов		**в**
1	− Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. О1 установки, настройки программных средств защиты информации в автоматизированной системе; О2 обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; О3 тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; О4 решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; О5 применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; О6 учёта, обработки, хранения и передачи информации, для которой установлен	Проверка отчета, дифференцированный зачет
2	− Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности		
3	− Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности		
4	− Составление документации по учету, обработке, хранению и передаче конфиденциальной информации		
5	− Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации		
6	− Составление маршрута и состава проведения различных видов контрольных		

	проверок при аттестации объектов, помещений, программ, алгоритмов.	режим конфиденциальности; О7 работы с подсистемами регистрации событий; О8 выявления событий и инцидентов безопасности в автоматизированной системе. **уметь:** У.1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных; У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; У.6 применять математический аппарат для выполнения криптографических преобразований; У.7 использовать типовые программные криптографические средства, в том числе электронную подпись; У.8 применять средства гарантированного уничтожения информации; У.9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У.10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. **знать**: З.1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	
7	– Устранение замечаний по результатам проверки		
8	– Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.		
9	– Применение математических методов для оценки качества и выбора наилучшего программного средства		
10	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.		

		З.2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; З.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; З.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации; З.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; З.6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	

Критерии оценки результатов освоения учебной практики

– **«5» «отлично» или «зачтено»** – студент показывает глубокое и полное овладение содержанием программного материала по УП, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

– **«4» «хорошо» или «зачтено»** – студент в полном объеме освоил программный материал по УП, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

– **«3» «удовлетворительно» или «зачтено»** – студент обнаруживает знание и понимание основных положений программного материала по УП но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения,

но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

– **«2» «неудовлетворительно» или «не зачтено»** – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по УП, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

.

4.2.2. Производственная практика:

Таблица 5

№ п/п	Виды работы на производственной практике	Содержание работ	Проверяемые результаты (ПК, ОК, ПО, У)	Форма про-верки ре-зультатов
1	Изучение инструкций по охране труда и технике безопасности	–Изучение инструкций по охране труда. Изучение инструкции по технике безопасности и пожароопасности, схем аварийных проходов и выходов. Изучение правил внутреннего распорядка правил и норм охраны труда, техники безопасности при работе с вычислительной техникой.	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных	Проверка отчета, дифференцированный зачет
2	Знакомство со структурой предприятия и видами его деятельности	– Знакомство со структурой и инфраструктурой организации, системой взаимоотношений между ее отдельными подразделениями, основными направлениями деятельности, отношениями с		

		партнерами.	событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. О1 установки, настройки программных средств защиты информации в автоматизированной системе; О2 обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; О3 тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; О4 решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; О5 применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; О6 учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; О7 работы с подсистемами регистрации событий; О8 выявления событий и инцидентов безопасности в автоматизированной системе. уметь: У.1 устанавливать, настраивать, применять	
3	Знакомство с системой защиты на предприятии	– Анализ принципов построения систем информационной защиты производственных подразделений		
4	Знакосмтво с программной и аппаратной системой защиты на предприятии	– Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.		
5	Диагностирование работоспособности программно-аппаратных средств	– Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;		
6	Эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности	– Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении		
7	Работа с конфиденциальной информацией	– Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации		

8	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности	– Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	программные и программно-аппаратные средства защиты информации; У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных; У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; У.6 применять математический аппарат для выполнения криптографических преобразований; У.7 использовать типовые программные криптографические средства, в том числе электронную подпись; У.8 применять средства гарантированного уничтожения информации; У.9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У.10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе	

			с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. знать: З.1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; З.2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; З.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; З.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации; З.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; З.6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	

Критерии оценки результатов освоения производственной практики

– **«5» «отлично» или «зачтено»** – студент показывает глубокое и полное овладение содержанием программного материала по УП, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в

форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

– **«4» «хорошо» или «зачтено»** – студент в полном объеме освоил программный материал по УП, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

– **«3» «удовлетворительно» или «зачтено»** – студент обнаруживает знание и понимание основных положений программного материала по УП но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

– **«2» «неудовлетворительно» или «не зачтено»** – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по УП, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

5. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (КОМ) ДЛЯ ЭКЗАМЕНА КВАЛИФИКАЦИОННОГО

5.1.Общие положения

КОМ предназначены для контроля и оценки результатов освоения профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами в рамках промежуточной аттестации по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

5.2. Задания для экзаменующихся

ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩИХСЯ № 1
количество вариантов 2

Типовое задание: разработка объектов по защите информации автоматизированных систем и предложения для работы с ней.
Оцениваемые компетенции: ОК 01-10, ПК 21.- 2.6.
Условия выполнения задания:

- экзамен по модулю осуществляется на базе ОГАПОУ «Алексеевский колледж» в учебной аудитории,
- используемое оборудование: персональный компьютер, программное обеспечение; нормативно- правовая документация.
- проверка задания осуществляется в цифровом и печатном виде.

Вариант задания № 1

Текст задания: Разработать информационную систему по защите информации автоматизированных систем в сберегательном банке.
Последовательность и условия выполнения задания:

В системе предусмотреть обработку следующих данных:

1) Информация о клиентах банка: Фамилия, имя отчество;
2) Информация о типах вкладов: Наименование, минимальный срок вклада, минимальная сумма вклада, валюта вклада, процентная ставка по вкладу;
3) Информация о сотрудниках банка, которые оформили вклады клиентов: Фамилия, Имя, Отчество, должность сотрудника.

Клиенты пользуются услугами банка по хранению своих денежных средств на различных вкладах, и получают проценты в соответствии с договором. Сотрудники банка оформляют вклады клиентов и заносят следующую информацию: ФИО клиента, вид вклада, дату

вклада, дату возврата вклада, сумму вклада, статус вклада (действующий, закрыт), ФИО сотрудника. Клиенты могут иметь несколько вкладов в банке. Сотрудники банка могут оформлять вклады разных клиентов.

4) Кроме того, в системе должна храниться информация об окладах, соответствующих занимаемым должностям сотрудников и обменный курс, соответствующей валюты.

Требования к интерфейсу программы.

1) Необходимо предусмотреть ввод, изменение и удаление данных в каждую таблицу только с помощью форм приложения. Можно использовать многостраничную форму.
2) При отображении данных из таблиц поля с внешними ключами не отображаются.
3) При вводе данных в подчиненные таблицы не должны отображаться коды ключевых полей.
4) Для минимум двух таблиц при добавлении или изменении значений использовать отдельную форму.
5) Предусмотреть обработку системных ошибок при изменении наборов данных.

Выполните запросы, которые предусмотрены заданием. Результат запросов отображать на отдельной вкладке.

Заполнить базу данными и подготовить тестовые примеры.

Информация для базы данных

Сотрудники банка и их должности

Фамилия	Имя	Отчество	Должности	Оклад
Иванов	Сергей	Владимирович	Менеджер	40000
Сергеева	Мария	Александровна	Экономист	50000
Кузнецова	Наталья	Сергеевна	Менеджер	40000
Петров	Сергей	Николаевич	Менеджер	40000
Крайнов	Александр	Владимирович	Бухгалтер	45000

Виды вкладов

	Наименование	Минимальный срок вклада, мес	Минимальная сумма вклада	Код_валюты	Процентная ставка, годовая
1	Накопительный	3	30000	рубль	8
2	Накопительный	3	500	доллар США	5
3	Накопительный	3	500	евро	4.5
4	Универсальный	12	50000	рубль	10
5	Универсальный	12	1000	доллар	4

				США	
6	Универсальный	12	1000	евро	3.5

Обменный курс валют

Наименование	Обменный курс
рубли	1
доллары США	60.85
евро	63.54

Клиенты банка

Фамилия	Имя	Отчество
Скворцов	Илья	Сергеевич
Петров	Игорь	Владимирович
Завьялова	Маргарита	Александровна
Жукова	Ирина	Сергеевна
Зайцев	Игорь	Сергеевич

Регистрация вкладов

Клиенты	Код вида вклада	Дата вклада	Дата возврата	Сумма вклада	Статус вклада	Сотрудник
Скворцов И.С.	1	25.03.15	26.04.16	40000	закрыт	Иванов С.В.
Петров И.В.	1	10.01.16	11.07.16	73000	закрыт	Кузнецова Н.С.
Завьялова М.А	4	15.01.16	16.01.17	100000	действует	Петров С.Н
Жукова И.С.	6	17.03.16	18.03.17	1200	действует	Иванов С.В.
Зайцев И.С.	1	17.01.16	18.09.16	250000	закрыт	Иванов С.В.
Скворцов И.С.	2	10.02.16	11.02.17	2000	действует	Кузнецова Н.С.
Петров И.В.	3	12.02.16	13.11.16	6000	закрыт	Кузнецова Н.С.
Завьялова М.А.	1	13.03.16	14.03.17	350000	действует	Кузнецова Н.С.
Петров И.В.	2	10.05.16	11.02.17	4000	действует	Иванов С.В.
Зайцев И.С.	4	14.05.16	15.05.17	150000	действует	Петров С.Н.

Максимальное время выполнения задания - 180 минут.

Вариант задания № 2

Текст задания: Разработать информационную систему по защите информации автоматизированных систем в магазине по прокату автомобилей.

Последовательность и условия выполнения задания:

Вам необходимо:

1) Разработать базу данных в соответствии со словарем данных.
2) Задать все первичные и внешние ключи, и другие ограничения.
3) Заполнить базу данными, которые находятся в файле Данные.xls.
4) Разработайте Windows-приложение. В приложении должны отображаться данные из всех таблиц. Для этого можно разработать отдельные формы или закладки. Данные должны отображаться в виде таблиц. Для отображения информации разработайте

представления. Внешние ключи в таблицах не должны отображаться.

5) На форме «Автомобили» отображается список автомобилей и их изображение. По списку можно перемещаться, просматривая автомобили.
6) Предусмотрите возможность ввода, изменения, удаления данных из таблиц. При удалении данных из таблиц, когда они используются в других таблицах выводить соответствующее сообщение.
7) Для заполнения таблицы Прокат разработать отдельную форму «Оформление заказа», которая открывается при нажатии на кнопку «Оформление заказа». Заказ оформляет Менеджер. Вводит дату выдачи, дату возврата, выбирает автомобиль из выпадающего списка (в списке отображаются только те автомобили, которые свободны в настоящее время) или форму со списком автомобилей, дополнительные услуги. Если клиент не обращался ранее, заполняет информацию о клиенте, а если обращался, то выбирает его из списка. После заполнения данных нажимает на кнопку «Рассчитать», происходит расчет стоимости заказа. Если клиент согласен, он вносит предоплату, или полную стоимость заказа. Менеджер вводит эту сумму в соответствующее поле формы, а также выбирает из списка свою фамилию, после нажимает на кнопку «Оформить заказ». Запись вводится в базу данных, а выбранный автомобиль переходит в состояние «заказан» (Поле Отметка о возврате принимает значение false).
8) При возвращении автомобиля Менеджер оформляет возврат автомобиля, для этого он выбирает соответствующую запись в таблице прокат и нажимает на кнопку «Оформить возврат» при этом выбранный автомобиль переходит в состояние «свободен» (Поле Отметка о возврате принимает значение true).
9) Разработайте документ «Заказ» в формате Excel, в котором должна отображаться информация (номер заказа, ФИО заказчика, Дата выдачи, Дата возврата, Дополнительные услуги, Стоимость Заказа, Фамилия Менеджера).
10) Разработайте дополнительные запросы и выведите информацию на форму. Сколько техосмотров провел каждый механик компании в 2017 году.
11) Заполните таблицу Прокат несколькими записями и сформируйте отчет общая стоимость заказов по месяцам.

Требования к интерфейсу программы.

6) Разработанные формы должны иметь приятный интерфейс, элементы форм должны быть выровнены, надписи должны быть выполнены без ошибок.
7) Предусмотреть обработку системных ошибок при изменении наборов данных.

Максимальное время выполнения задания - 180 минут.

5.3. Перечень материалов и оборудования, допущенных к использованию на экзамене по модулю

Основные источники:

1. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

2. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.

3. Криптографическая защита информации в объектах информационной инфраструктуры:учебник, 1-е изд.,/ Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - ИЦ Академия, 2020 -288 с.

4. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.

Дополнительные источники:

1. Гвоздева В. А. Информатика, автоматизированные информационные технологии и системы. Учебник.- М.: ИД ФОРУМ, 2017.- 544 с.

2. Гришин В.Н., Панфилова Е. Е. Информационные технологии в профессиональной деятельности: учебник. – М.: ИД «Форум»: ИНФРА-М, 2010. -416 с.: ил. - (Профессиональное образование).

3. Михеева Е.В. Информационные технологии в профессиональной деятельности: учебник/Е.В. Михеева. – 13-е изд., стер. – М.: Академия, 2014. –

384 с.
4. Михеева Е.В. Практикум по информационным технологиям в профессиональной деятельности: учебник/Е.В. Михеева. – 14-е изд., стер. – М.: Академия, 2014.
5. Федотова Е. Л. Информационные технологии в профессиональной деятельности: учебное пособие. - М.: ИД «Форум»: ИНФРА-М, 2014.- 368 с.: ил. - (Профессиональное образование).

Электронные издания (электронные ресурсы):

1. **Цифровая образовательная среда СПО PROFобразование:**

– Лебедева, Т. Н. Информатика. Информационные технологии : учебно-методическое пособие для СПО / Т. Н. Лебедева, Л. С. Носова, П. В. Волков. — Саратов : Профобразование, 2019. — 128 c. — ISBN 978-5-4488-0339-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/86070 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. Пользователей

– Аникеева, Л. А. Лабораторные работы по Excel / Л. А. Аникеева. — Москва : СОЛОН-ПРЕСС, 2019. — 112 c. — ISBN 978-5-91359-257-6. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/90300 (дата обращения: 02.09.2020). — Режим доступа: для авторизир. Пользователей

– Аникеева, Л. А. Упражнения по текстовому редактору Word / Л. А. Аникеева. — Москва : СОЛОН-ПРЕСС, 2019. — 119 c. — ISBN 978-5-91359-084-8. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/90385 (дата обращения: 01.08.2020). — Режим доступа: для авторизир. Пользователей

– Клочко, И. А. Информационные технологии в профессиональной деятельности : учебное пособие для СПО / И. А. Клочко. — 2-е изд. — Саратов : Профобразование, Ай Пи Эр Медиа, 2019. — 292 c. — ISBN 978-5-4486-0407-2, 978-5-4488-0219-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/80327 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. Пользователей

Электронно-библиотечная система:

IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

5.4. Пакет экзаменатора

5.4.1. Организация экзамена по модулю

Номер и краткое содержание задания	Коли чество вариант ов зада ний	Время выполн ения задания	Оцени ваемые компе тенции	Показатели оценки результата
Типовое задание: разработка объектов по защите информации автоматизированных систем и предложения для работы с ней.	2	180 мин.	ОК 01-10, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6.	Проверка задания осуществляется в цифровом и печатном виде по критериям: 1. Разработана база данных 2. База данных нормализована и приведена к третьей нормальной форме

Условия для выполнения заданий:

– экзамен по модулю осуществляется на базе ОГАПОУ «Алексеевский колледж» в учебной аудитории,

– используемое оборудование: персональный компьютер, программное обеспечение; нормативно- правовая документация.

– Требования охраны труда: инструктаж по технике безопасности.

Литература для экзаменующихся:

Основные источники:

5. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

6. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.

7. Криптографическая защита информации в объектах информационной инфраструктуры:учебник, 1-е изд.,/ Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - ИЦ Академия, 2020 -288 с.

8. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.

Дополнительные источники:

6. Гвоздева В. А. Информатика, автоматизированные информационные технологии системы. Учебник.- М.: ИД ФОРУМ, 2017.- 544 с.

7. Гришин В.Н., Панфилова Е. Е. Информационные технологии в профессиональн деятельности: учебник. – М.: ИД «Форум»: ИНФРА-М, 2010. -416 с.: ил. (Профессиональное образование).

8. Михеева Е.В. Информационные технологии в профессиональной деятельност учебник/Е.В. Михеева. – 13-е изд., стер. – М.: Академия, 2014. –384 с.

9. Михеева Е.В. Практикум по информационным технологиям в профессиональной деятельности: учебник/Е.В. Михеева. – 14-е изд., стер. – М.: Академия, 2014.
10. Федотова Е. Л. Информационные технологии в профессиональной деятельности: учебное пособие. - М.: ИД «Форум»: ИНФРА-М, 2014.- 368 с.: ил. - (Профессиональное образование).

Электронные издания (электронные ресурсы):

2. Цифровая образовательная среда СПО PROFобразование:

– Лебедева, Т. Н. Информатика. Информационные технологии : учебно-методическое пособие для СПО / Т. Н. Лебедева, Л. С. Носова, П. В. Волков. — Саратов : Профобразование, 2019. — 128 c. — ISBN 978-5-4488-0339-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/86070 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. Пользователей

– Аникова, Л. А. Лабораторные работы по Excel / Л. А. Аникова. — Москва : СОЛОН-ПРЕСС, 2019. — 112 c. — ISBN 978-5-91359-257-6. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/90300 (дата обращения: 02.09.2020). — Режим доступа: для авторизир. Пользователей

– Аникова, Л. А. Упражнения по текстовому редактору Word / Л. А. Аникова. — Москва : СОЛОН-ПРЕСС, 2019. — 119 c. — ISBN 978-5-91359-084-8. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/90385 (дата обращения: 01.08.2020). — Режим доступа: для авторизир. Пользователей

– Клочко, И. А. Информационные технологии в профессиональной деятельности : учебное пособие для СПО / И. А. Клочко. — 2-е изд. — Саратов : Профобразование, Ай Пи Эр Медиа, 2019. — 292 c. — ISBN 978-5-4486-0407-2, 978-5-4488-0219-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/80327 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. Пользователей

Электронно-библиотечная система:

IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

Рекомендации по проведению оценки:
1. Ознакомить с заданиями для экзаменующихся, оцениваемыми компетенциями и показателями оценки.
2. Определить основную и дополнительную литературу, необходимую для оценивания.
3. Создать доброжелательную обстановку.
4. Не вмешиваться в ход выполнения задания.

5.4.2. Критерии оценки результатов освоения профессионального модуля

Коды и наименования проверяемых компетенций или их сочетаний	Показатели оценки результата	Оценка (да / нет)
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и	

использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

Решение «вид профессиональной деятельности освоен» принимается если:

1) задание выполнено в полном объеме;

2) работа отличается глубиной проработки всех вопросов содержательной части;

3) студент свободно владеет теоретическим материалом, на все вопросы дает правильные и обоснованные ответы либо студент твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя и на большинство вопросов даны правильные ответы;

4) студент убедительно защищает свою точку зрения либо студент защищает свою точку зрения достаточно обоснованно;

5) студент обращался в ходе выполнения задания к нормативно-правовым актам;

6) студент рационально распределил время на выполнение задания по этапам: ознакомление с заданием и планирование работы, распределение времени на выполнение элементов задания; получение и поиск необходимой информации; демонстрация последовательности выполнения работы;

7) осуществлялась рефлексия выполнения задания и коррекция подготовленных документов перед сдачей;

8) задания выполнены самостоятельно и своевременно (в соответствии с установленным лимитом времени).

Решение «вид профессиональной деятельности не освоен» принимается если студент допустил грубые фактические ошибки при выполнении задания, не дает ответа на поставленные вопросы, не может отстоять свою точку зрения.

6. ДОКУМЕНТЫ, ОТРАЖАЮЩИЕ РЕЗУЛЬТАТЫ УСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
программы подготовки специалистов среднего звена
по специальности СПО
10.02.05 Обеспечение информационной безопасности автоматизированных систем

ОГАПОУ «Алексеевский колледж»
ЭКЗАМЕНАЦИОННАЯ ВЕДОМОСТЬ

Группа _____

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
Дисциплина МДК 02.01. Программные и программно-аппаратные средства защиты информации
Дата экзамена (зачета, д/зачета) _____
Начало экзамена (зачета, д/зачета) _____ Окончание экзамена (зачета, д/зачета)_____
Экзаменатор_____
(фамилия, имя, отчество)

№ п/п	Фамилия, имя, отчество	№ экзам. билета	оценка (цифрой, прописью)	подпись экзаменатора
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				

Всего сдавали экзамен (зачет, д/зачет) _____человек, из них получили оценки:

Оценки	Кол-во	%
«5»		
«4»		
«3»		
«2»		

Средний балл _____
Показатель качества знаний_____

ОГАПОУ «Алексеевский колледж»
ЭКЗАМЕНАЦИОННАЯ ВЕДОМОСТЬ

Группа _____

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
Дисциплина МДК 02.02. Криптографические средства защиты информации
Дата экзамена (зачета, д/зачета) _____
Начало экзамена (зачета, д/зачета) _____ Окончание экзамена (зачета, д/зачета)_____
Экзаменатор_____
(фамилия, имя, отчество)

№ п/п	Фамилия, имя, отчество	№ экзам. билета	оценка (цифрой, прописью)	подпись экзаменатора
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				

Всего сдавали экзамен (зачет, д/зачет) _____человек, из них получили оценки:

Оценки	Кол-во	%
«5»		
«4»		
«3»		
«2»		

Средний балл _____
Показатель качества знаний_____

ОГАПОУ «Алексеевский колледж»
ЭКЗАМЕНАЦИОННАЯ ВЕДОМОСТЬ

Группа _____

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
Дисциплина УП.02. Учебная практика по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Дата экзамена (зачета, д/зачета) _____
Начало экзамена (зачета, д/зачета) _____ Окончание экзамена (зачета, д/зачета)_____
Экзаменатор_____
(фамилия, имя, отчество)

№ п/п	Фамилия, имя, отчество	№ экзам. билета	оценка (цифрой, прописью)	подпись экзаменатора
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				

Всего сдавали экзамен (зачет, д/зачет) _____человек, из них получили оценки:

Оценки	Кол-во	%
«5»		
«4»		
«3»		
«2»		

Средний балл _____
Показатель качества знаний_____

_____ _____
(подпись) (расшифровка)

ОГАПОУ «Алексеевский колледж»
ЭКЗАМЕНАЦИОННАЯ ВЕДОМОСТЬ

Группа _____

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
Дисциплина ПП.02. Производственная практика по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Дата экзамена (зачета, д/зачета) _____
Начало экзамена (зачета, д/зачета) _____ Окончание экзамена (зачета, д/зачета)_____
Экзаменатор_____
(фамилия, имя, отчество)

№ п/п	Фамилия, имя, отчество	№ экзам. билета	оценка (цифрой, прописью)	подпись экзаменатора
26.				
27.				
28.				
29.				
30.				
31.				
32.				
33.				
34.				
35.				
36.				
37.				
38.				
39.				
40.				
41.				
42.				
43.				
44.				
45.				
46.				
47.				
48.				
49.				
50.				

Всего сдавали экзамен (зачет, д/зачет) _____человек, из них получили оценки:

Оценки	Кол-во	%
«5»		
«4»		
«3»		
«2»		

Средний балл _____
Показатель качества знаний_____

_____ _____
(подпись) (расшифровка)

ОГАПОУ «Алексеевский колледж»
ВЕДОМОСТЬ ЭКЗАМЕНА ПО МОДУЛЮ

Результаты освоения ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Наименование

по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем_____

№	Ф.И.О. студента	№ билета	Результаты аттестации		УП 02. Учебная практика	ПП.02 Производственная практика	ПК	Экзамен (одулю) оценка	Подпись
			Мдк 02.01	Мдк 02.02			од ПК 2.1.- 2..6		
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									

Оценка	5	4	3	2	н/а	Средний балл	Качествен. показатель
Кол-во							

Председатель комиссии _____
Члены комиссии _____
_____
Дата _____г.

ПЕРЕЧЕНЬ

формируемых профессиональных компетенций

ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Аттестационный лист по учебной практике

студент(ка) _____
обучающийся(аяся) на ____ курсе по специальности/профессии СПО

_____
код и наименование

успешно прошел(ла) учебную практику _____по профессиональному модулю
наименование практики в соответствии с учебным планом

_____
наименование профессионального модуля

в объеме _____ часов с_____ по_____
в

_____
наименование организации, юридический адрес

1. Виды и качество выполнения работ в период производственной практики

Виды и объем работ, выполненных обучающимся во время практики	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика (оценка)

2. За время практики обучающийся проявил личностные и деловые качества

Проявленные личностные и деловые качества		Степень проявления		
		Не проявлял	Проявлял эпизодически	Проявлял регулярно
1	Понимание сущности и социальной значимости профессии			
2	Проявление интереса к профессии			
3	Ответственное отношение к выполнению порученных производственных заданий			
4	Самооценка и самоанализ выполняемых действий			
5	Способность самостоятельно принимать решения			
6	Поиск, анализ и оценка информации, необходимой для постановки и решения профессиональных задач			
7	Использование информационно-коммуникационных технологий при освоении вида профессиональной деятельности			
8	Способность работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями			
9	Способность самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием			

3. За время прохождения практики у обучающегося были сформированы компетенции

№	Перечень общих и профессиональных компетенций	Компетенция (элемент компетенции)
		Сформирована (не сформирована)
1. Общие компетенции		

1		
2		
3		

2. Профессиональные компетенции

№	Код и формулировка ПК	Основные показатели оценки результата	Компетенция (элемент компетенции)
			Сформирована (не сформирована)
1			
2			
3			

Дата «___»_____ 20__г

Подпись руководителя подгруппы (куратора) _____/ФИО, должность

Подпись руководителя подгруппы (наставника)_____ /ФИО, должность

Подпись руководителя ПОО _____/ФИО, должность

МП

Аттестационный лист по производственной практике

студент(ка) _____
обучающийся(аяся) на ____ курсе по специальности/профессии СПО

_____
код и наименование

успешно прошел(ла) производственную практику _____по профессиональному модулю
наименование практики в соответствии с учебным планом

_____
наименование профессионального модуля

в объеме _____ часов с_____ по_____
в

_____
наименование организации, юридический адрес

1. Виды и качество выполнения работ в период производственной практики

Виды и объем работ, выполненных обучающимся во время практики	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика (оценка)

2. За время практики обучающийся проявил личностные и деловые качества

Проявленные личностные и деловые качества		Степень проявления		
		Не проявлял	Проявлял эпизодически	Проявлял регулярно
1	Понимание сущности и социальной значимости профессии			
2	Проявление интереса к профессии			
3	Ответственное отношение к выполнению порученных производственных заданий			
4	Самооценка и самоанализ выполняемых действий			
5	Способность самостоятельно принимать решения			
6	Поиск, анализ и оценка информации, необходимой для постановки и решения профессиональных задач			
7	Использование информационно-коммуникационных технологий при освоении вида профессиональной деятельности			
8	Способность работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями			
9	Способность самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием			

3. За время прохождения практики у обучающегося были сформированы компетенции

№	Перечень общих и профессиональных компетенций	Компетенция (элемент компетенции)
		Сформирована (не сформирована)
1. Общие компетенции		
1		
2		

3		
4		

2. Профессиональные компетенции

№	Код и формулировка ПК	Основные показатели оценки результата	Компетенция (элемент компетенции)
			Сформирована (не сформирована)
1			
2			
3			

Дата «___»_____ 20__г

Подпись руководителя подгруппы (куратора) _____/ФИО, должность

Подпись руководителя подгруппы (наставника)_____ /ФИО, должность

Подпись руководителя предприятия _____/ФИО, должность

МП

ПРОИЗВОДСТВЕННАЯ ХАРАКТЕРИСТИКА

обучающегося _____ группы специальности / профессии

_____

код и наименование

ОГАПОУ «Алексеевский колледж»

_____

ФИО обучающегося

Студент(ка) с _____ по _____ г. проходил(а) производственную практику по ПМ _____

в_____.

В период производственной практики студент(ка) познакомился(лась) со структурой и организацией работы учреждения, изучила обязанности работников в основных подразделениях учреждения и выполняла работы в соответствии с программой практики и по заданию руководителя практики от предприятия.

Практикант(ка) выполнял (а) следующие виды работ:

_____.

виды работ

Практикант(ка) успешно применял(а) полученные в Колледже теоретические знания и умения в области_____,

указываются области профессиональной деятельности в соответствии с ВПД/ВД/ОВД

углубляя и закрепляя их в процессе производственной практики.

Студент(ка) продемонстрировал(а), _____,

указывается уровень сформированности профессиональных компетенций (высокий/средний/низкий)

уровень сформированности следующих профессиональных компетенций: _____.

указывается наименование профессиональных компетенций в соответствии с программой практики

За период практики студент(ка) продемонстрировал(а), _____,

указывается уровень сформированности общих компетенций (высокий/средний/низкий)

уровень сформированности следующих общих компетенций: _____.

указывается наименование общих компетенций в соответствии с программой практики

Студент(ка) полностью выполнил(а) задания, предусмотренные программой производственной практики, ежедневно отражал(а) в дневнике и отчете анализ выполненных работ, соблюдал(а) действующие в учреждении правила внутреннего трудового распорядка, изучил(а) и строго соблюдал(а) правила охраны труда, техники безопасности и производственной санитарии.

Материалы по результатам прохождения производственной практики выполнены на хорошем уровне и заслуживают положительной оценки. Вид профессиональной деятельности _____ студент(ка) освоил(а).

указывается наименование ВПД/ВД/ОВД

Куратор практики _____ _____, преподаватель ОГАПОУ «Алексеевский колледж»

Наставник _____ _____ , _____

подпись расшифровка должность

Руководитель предприятия _____ _____, _____

подпись расшифровка должность

МП

_____ г.